FIPS 201 Evaluation Program - Laboratory Qualification Procedures & Requirements

Version 1.0.0
April 12, 2007

Document History

Status	Version	Date	Comment	Audience
Approved	1.0.0	04/12/07	Initial version	Public

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to define requirements and procedures for Laboratories that show interest in performing evaluations of Product/Services on behalf of the General Services Administration (GSA). This document sets forth the requirements and procedures under which the FIPS 201 Evaluation Program qualifies Laboratories to determine a Product/Service compliance with FIPS 201 requirements.

1.2 Scope

This document is for use by Laboratories in understanding the managerial/technical requirements for evaluating products/services for compliance with FIPS 201 and supporting documents. Laboratory customers may also use it as a basis upon which to judge the competence of Laboratories.

1.3 Background

Homeland Security Presidential Directive-12 (HSPD-12), "*Policy for a Common Identification Standard for Federal Employees and Contractors*" establishes the requirement for a mandatory Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors. The Office of Management and Budget (OMB) has designated the GSA as the Executive Agent for Government-wide acquisitions for the implementation of HSPD-12. OMB has directed Federal Agencies to purchase only products and services that are compliant with the Federal policy, standards and numerous supporting technical specifications.

To ensure standard HSPD-12 compliant products and services are available, NIST has issued requirements in FIPS 201 and supporting documentation (http://csrc.nist.gov/piv-program/fips201-support-docs.html).

As mandated by OMB through M05-24, GSA has been designated as the "executive agent for Government-wide acquisitions of information technology" under section 5112(e) of the Clinger-Cohen Act of 1996 (40 U.S.C. Sec. 11302(e)) for the products and services required by the HSPD-12. GSA will ensure all approved Suppliers provide products and services that meet all applicable federal standards and requirements through fully operational Laboratories under the FIPS 201 Evaluation Program.

The GSA FIPS 201 Evaluation Program is currently set up to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. Twenty-one product/service categories were created using FIPS 201 and supporting documentation as the foundation. Each category has developed approval and test procedures which outline the evaluation criteria, approval mechanisms and test process employed by the Laboratory during their evaluation of a Supplier's product or service against the requirements for that category. The initial cost of evaluating each product was funded by GSA. As of April 4, 2007, individually qualified Laboratories will be charging fees to the applicants for evaluation services

1.4 Description of the FIPS 201 Evaluation Program

The FIPS 201 Evaluation Program is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. A goal of the FIPS 201 Evaluation Program (EP) is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. A set of approval and test procedures have been developed which outline the evaluation criteria, approval mechanisms and test process employed by the Laboratory during their evaluation of a Supplier's product or service against the requirements for that category.

Once evaluated and approved by GSA, products and services are placed on the FIPS 201 Approved List. Agencies can then procure these products and services from Suppliers for their HSPD-12 implementations having full assurance that they meet all the requirements of FIPS 201 and all supporting documentation.

The EP was developed in 3 stages. The primary goal of the first stage was to determine which card /reader requirements are deemed necessary in order to achieve interoperability between Government facilities. The second stage designed, developed, but did not implement a model modular Laboratory. The third stage instantiated an operational modular Laboratory in contractors' facilities. The third stage validated the modular concept designed in the second stage. This concept (defined in the [LAB SPEC]) will be used by all Applicant Laboratories in the completion of FIPS 201 EP product/service evaluations.

1.4.1 EP Information

The EP makes the following information publicly available through its Website - <http://www.fips201ep.cio.gov>:

a) A description of the EP categories;

b) A directory of EP qualified Laboratories; which includes the name and address, qualification effective and expiration dates;

c) EP Lab Qualification Site Visit checklists;

d) The Laboratory Specification describing required Laboratory components and processes to be followed;

e) The Approval and Test Procedures for all EP categories; and

f) Various publications and forms for the use and benefit of EP qualified Laboratories, EP Assessors, and technical experts, and other interested parties.

1.5 GSA Lab Qualification Policy

EP Laboratories (EPLs) are established to meet demonstrated needs, based on requests for service. The specific evaluation processes employed by each qualified Laboratory is defined by predefined EP Approval and Test Procedures.

The EP administers its policies and procedures in a completely impartial manner. Access to EP qualification is only conditional on prior accreditation as a NIST PIV NVLAP. It is not conditional on the size of a Laboratory or on its membership in any association or group, nor is it conditional upon the number of Laboratories already qualified. EP qualification services are available to public and private testing Laboratories , including commercial Laboratories , manufacturers' in-house Laboratories , university Laboratories , and federal, state, and local government Laboratories . However, it is a pre-qualification requirement that only NIST accredited NVLAP Laboratories can be qualified to serve as a GSA FIPS 201 Evaluation Program Laboratory and that all qualified labs are located in North America.

EP Laboratory qualification is based on evaluation of a Laboratory's management and technical qualifications, and competence for conducting predefined Approval and Test Procedures. Qualification is granted only after thorough evaluation of an applicant has demonstrated that all EP requirements have been fulfilled, and is acknowledged by the issuance of a Qualification Statement generated by the EP.

EP Qualification does not relieve a Laboratory from complying with applicable federal, state, and local laws and regulations.

1.6 References

The following is a list of references used to develop this document.

[HSPD-12] HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* August 27, 2004.
http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

[FIPS 201] NIST FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* NIST, March 2006.
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-v5.pdf

[SP 800-18] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems,* Revision 1, February 2006.
http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

[SP 800-53] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* February 2005.
http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[SP 800-73] NIST Special Publication 800-73, *Interfaces for Personal Identity Verification,* NIST, April 2005.
http://csrc.nist.gov/publications/nistpubs/800-73/SP800-73-Final.pdf

[SP 800-76] NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification,* NIST, February 2005.
http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf

[SP 800-78] NIST Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification,* NIST, April 2005.

http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

[SP 800-79] NIST Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, NIST, July 2005.
http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf

[EP] NIST Handbook 150, 2001 Edition, *Procedures and General Requirements Handbook*, July 2001.
http://ts.nist.gov/ts/htdocs/210/214/docs/nist-handbook-150.pdf

[LAB SPEC] *FIPS 201 Evaluation Program -Laboratory Specificatio*n, May 17 2006.
http://fips201ep.cio.gov/documents/Lab_Specification_v2_0_0.pdf

[CONFIG PLAN] *FIPS 201 Evaluation Program Development -Configuration Management Plan*
http://fips201ep.cio.gov/documents/CM_Plan_v2_0_0.pdf

1.7 Terms and Definitions

For the purposes of this handbook, these relevant terms and definitions apply:

1.7.1 Qualification

The process by which a GSA Government representative validates an organization's ability to perform FIPS 201 evaluations.

1.7.2 Applicant Laboratory

An organization that is committed to achieving the required management and technical processes and expertise mandated by the EP to successfully evaluate products & services for compliance with FIPS 201 documentation.

1.7.3 Category

A profile for each FIPS 201 product or service that is acceptable for evaluation. Each category specifies the complete list of requirements specific to it, and the relevant approval mechanisms. Each category's requirements set (i.e., category-specific requirements) influences the approval process and the evaluation process. There is one Approval Procedure per category, customized as appropriate for the category-specific requirements.

1.7.4 Supplier Applicant

A supplier who submits a formal application to have their product or service evaluated for conformance to category-specific requirements.

1.7.5 Approval Mechanisms

Specific tools and other mechanisms used during the evaluation process. This includes, but is not limited to supplier attestation forms, Lab Test Data Report, and site visits. Each Approval Procedure document specifies the approval mechanisms relevant to its set of requirements.

1.7.6 Approval Procedures

The specific steps and actions specified in the Approval Procedure documents, and further detailed in the Lab Specification. Approval Procedures pertain to the end-to-end process that includes all the phases cited in the Approval Process definition.

1.7.7 Approval Process

The overall, end-to-end sequence of events involved with a Lab addressing a supplier product or service. The effort is multi-phased. The phases are (1) application, (2) evaluation, (3) evaluation report generation, (4) notification, and (5) an optional non-conformance review. The desired result of the Approval Process is the addition of a FIPS 201 conformant product or service to the Approved FIPS 201 Products and Services List.

1.7.8 Category

Profile for each FIPS 201 product or service the Lab will accept for evaluation. Each category specifies the complete list of requirements specific to it, and the relevant approval mechanisms. Each category's requirements set (i.e., category-specific requirements) influences the approval process (to a small degree) and the evaluation process (to a large degree). There is one Approval Procedure per category, customized as appropriate for the category-specific requirements.

1.7.9 Evaluation Procedures

The specific steps and actions specified in each Approval Procedure document pertaining specifically to product or service evaluation. Each Approval Procedure document specifies the evaluation procedures relevant to its set of requirements.

1.7.10 Customer

Any person or organization that engages the services of an EP Qualified Laboratory.

1.7.11 Competence

Ability of a Laboratory to conduct tests and perform calibrations in accordance with the specified standards and to produce accurate, proper, fit for purpose, technically valid data and test and calibration results.

1.7.12 Laboratory

Organization that performs electronic test on products, and evaluation of supplier applicant data. When a Laboratory is part of an organization that carries out activities additional to electronic test on products, and evaluation of supplier applicant data, the term Laboratory refers only to those parts of that organization that are involved in the evaluation process.

1.7.13 Role Qualification Traceability Matrix Worksheet

A worksheet submitted as part of the Applicant Lab's application that provides justification for each required element defined in each role described in the [LAB SPEC]. The worksheet is completed by each applicant lab.

1.8 Confidentiality

To the extent permitted by applicable laws, GSA will protect the confidentiality of all information obtained relating to the application, on-site assessment, proficiency testing, evaluation, and qualification of Laboratories.

In addition, the EP and the Laboratory seeking qualification acknowledge and agree that the qualification assessments and work done by the EP is done in accordance with the authority granted to GSA by OMB memo M05-24.The EP and the Laboratory further agree that to the extent permitted by law, GSA will protect information obtained during application, on-site assessment, proficiency testing, evaluation, and qualification from disclosure pursuant to Title 15 USC 3710a(c)(7)(A) and (7)(B) for a period of five years after it is obtained.

1.9 Complaints

A complaint regarding the activities of the EP or of an EP qualified Laboratory may be lodged by any person or organization. Information about the complaint should be put in writing and mailed, faxed, or e-mailed to the EP (april.giles@gsa.gov), along with supporting documentation, if available. A complaint concerning an EP qualified Laboratory should first be addressed by the Laboratory against which the complaint is lodged.

2 Qualification Process

Any Laboratory may apply for qualification by the EP. The Laboratory must demonstrate competence in all categories. If additional categories are added then the Laboratory must demonstrate competence in the new categories to maintain qualification status. In order to initiate the qualification process, the Applicant Laboratory shall submit a completed application along with a quality manual and relevant associated documentation, agree to conditions for qualification, and pay any required fees. It is a pre-qualification requirement that only NIST accredited NVLAP Laboratories can be qualified to serve as a GSA FIPS 201 Evaluation Program Laboratory.

2.1 Request an Application Package

An Applicant Laboratory shall make written request for an application package from the EP. The request shall be emailed to April.Giles@gsa.gov.

2.2 Submit an Application Package

2.2.1 An Applicant Laboratory shall complete an application package for qualification that includes the following information:

a) The legal name and full address of the Laboratory;
b) The ownership of the Laboratory;
c) The Authorized Representative's (must be "C" level, President, or Vice President) name and contact information;
d) The names, titles, contact information, resume, and role qualification traceability matrix worksheet (as shown in Section 3) for Laboratory staff nominated to serve in each role defined by the EP Laboratory Specification;
e) An organizational chart depicting roles defined in EP Laboratory Specification;
f) A general description (limit 1 page) of the Laboratory, including its facilities and scope of operation;
g) A copy of NIST Personal Identity Verification Program (NPIVP) Certificate of Qualification;
h) A signed copy of EP Laboratory Specification Rules of Behavior (sample shown in Appendix A) from each Laboratory staff member.
i) The Laboratory's Authorized Representative (must be "C" level, President, or Vice President) signed & notarized conditions for qualification form (sample shown in Appendix B);
j) A signed statement from each proposed lab staff member that they have read/understand the EP Laboratory Specification, and agree to perform evaluation tasks as prescribed.

2.3 Review of Application

Upon receipt of a Laboratory's application for qualification, the EP assigns a priority code to the Applicant Laboratory; acknowledges receipt of the application in writing (via email); reviews the information supplied by the Laboratory for adequacy; requests further information, if necessary; and specifies the next step(s) in the qualification process.

2.4 Assignment of Assessor(s)

The EP selects Assessors on the basis of their professional and academic achievements, experience in the field of testing, management experience, training, technical knowledge, and communications skills.

The EP assigns qualified Assessors to evaluate all information collected from an Applicant Laboratory and to conduct the assessment on its behalf at the Laboratory and any other sites where activities to be covered by the qualification are performed.

2.5 Document Review

The EP Assessor(s) assigned to an assessment reviews all documents submitted with the application to ensure they satisfy the requirements in this handbook. The EP assessor may ask for additional management system documents and/or records in order to facilitate the review.

The EP Assessor may identify nonconformities in the documentation. Nonconformities are discussed with the Authorized Representative and the Laboratory must address them prior to the on-site assessment. The assessor will provide a list of the nonconformities to the Laboratory in writing. Where the documentation requires significant revision, the EP will require that the Laboratory improve its documentation and submit it for further review prior to proceeding with the qualification process.

2.6 Scheduling the On-site Assessment

The Applicant Laboratory is contacted by the Assessor to schedule a mutually acceptable date for the on-site assessment. An assessment normally takes one to three days. Every effort is made to conduct an assessment with as little disruption as possible to the normal operations of the Laboratory.

If a Laboratory requires that its established assessment date be changed, it shall contact the Assessor(s) and the EP. The Laboratory is responsible for any costs associated with the date change.

Following initial qualification, an on-site assessment will be conducted during the first renewal year, and every two years thereafter. Delay of assessments beyond these frequencies may affect the Laboratory’s qualification status.

2.7 Conducting the On-site Assessment

An on-site assessment is conducted at all Applicant Laboratory locations where evaluations will be performed. Assessors use checklists provided by the EP so that each Laboratory receives an assessment comparable to that received by others. Checklists are normative documents that include and expand upon the requirements outlined in this document.

Prior to the assessment, and after successful completion of the documentation review stage, the Applicant Laboratory will be given access to the Web-Enabled Tool, the web-enabled tool manual, and necessary product for at least one trial evaluation to complete, and demonstrate during the on-site assessment.

At the beginning of the assessment, an opening meeting is conducted with management and Laboratory personnel to explain the purpose of the on-site assessment and to discuss the schedule for the assessment activities.

During the assessment, the Assessor examines the management system, reviews quality and technical records, examines equipment and facilities, interviews staff, observes demonstrations of evaluations (including use of Web-Enabled Tool), and examines sample trial evaluation reports (created from trial evaluation).

In order to conduct an appropriate assessment of competence, the Assessor requires access to Laboratory records for all staff members who routinely perform, or affect the quality of FIPS 201 Product/Service evaluations. This includes resumes, job descriptions of key personnel, training, and competency evaluations. The Assessor need not be given information that violates individual privacy, such as salary, medical information, or performance reviews outside the scope of the qualification program.

At the conclusion of the assessment, the Assessor conducts a closing meeting to discuss observations and any nonconformity with the Authorized Representative and other responsible Laboratory staff.

2.8 Completing the On-site Assessment Report

Within 5 days of the on-site assessment, the Assessor submits a written report on the compliance of the Applicant Laboratory with the qualification requirements. The report shall include as a minimum:

a) The date(s) of assessment;
b) The names of the Assessor(s) responsible for the report;
c) The names and addresses of all the Laboratory sites assessed;
d) Comments and/or nonconformities cited by the Assessor(s) on the compliance of the Applicant Laboratory with the qualification requirements; and
e) A copy of completed checklists.

The Authorized Representative signs the report to acknowledge that the Assessor has discussed its content and agrees to respond to the EP regarding resolution of nonconformities within 10 days (see 2.9).

The Assessor forwards the original report to the EP.
The EP is responsible for the content of the on-site assessment report, including the stating of nonconformities.

2.9 Nonconformity Notification and Resolution

An Applicant Laboratory is informed of nonconformities during the on-site assessment, and nonconformities are documented in the on-site assessment report.

A Laboratory shall respond in writing to the EP within ten (10) days of the date of the on-site assessment report, addressing all documented nonconformities. The response shall be signed by the Authorized Representative and shall include documentation that the specified

nonconformities have either been corrected or will be corrected as described in a plan of corrective actions. A corrective action plan must include a list of actions, target completion dates, and names of persons responsible for discharging those actions.

All nonconformities shall be satisfactorily resolved before initial qualification may be granted. Should resolution take longer than 10 days, the Laboratory may submit a corrective action plan in its initial response, and provide evidence of resolution when the planned actions have been completed. At that time, the EP will continue with the qualification process.

Once qualification has been granted, nonconformities affecting the outcome of tests or calibrations shall be addressed and corrected within the 10-day limit. Evidence shall be supplied which clearly demonstrates that actions taken fully resolve the nonconformities, thereby removing any concern as to the quality of results of the tests or calibrations conducted by the Laboratory. Should resolution take longer than 10 days, the Laboratory's qualification may be subject to adverse action. In those cases where nonconformities do not directly affect the results of FIPS 201 Product/Service evaluations, such as those related to record-keeping, the EP, at its discretion, may accept a plan of corrective action as satisfactory resolution. When this occurs, Laboratories are expected to submit sufficient objective evidence to demonstrate that the nonconformities have been resolved according to the plan.

When responding to nonconformities, the Laboratory shall reference each nonconformity by the item number shown on the on-site assessment checklist.

The Laboratory may ask for clarification of a nonconformity from either the Assessor during the closing meeting or the appropriate the EP Program Manager at any time. A Laboratory may also challenge the validity of a nonconformity by writing to the EP Program Manager.

If substantial nonconformities are cited, the EP may require an additional on-site assessment prior to granting qualification. All nonconformities and resolutions will be subject to thorough review and evaluation prior to a qualification decision.

2.10 Qualification Decision

The EP Program Manager is responsible for all EP qualification actions, including granting, renewing, suspending, and revoking any EP qualification.
The qualification decision is based on EP review of information gathered during the qualification process and a determination of whether or not all requirements for qualification have been fulfilled.
The evaluation process considers the Laboratory's record as a whole, including:

a. The information provided on the application;
b. The results of documentation review;
c. The on-site assessment reports;
d. The actions taken by the Applicant Laboratory to correct nonconformities; and
e. The results of trial evaluation.

Based on this evaluation, the EP determines whether or not the Applicant Laboratory should be qualified. If the evaluation reveals nonconformities beyond those identified in the assessment process, EP will inform the Laboratory in writing of the nonconformities, and the Laboratory

shall respond as specified in Section 2.9. All nonconformities must be resolved to EP's satisfaction before qualification can be granted.

2.11 Granting Lab Qualification

2.11.1 Qualification without Restrictions

Initial qualification is granted when a Laboratory has met all EP requirements. One of four qualification renewal dates (January 1, April 1, July 1, or October 1) is assigned to the Laboratory and is usually retained as long as the Laboratory remains in the program. The renewal period is one year; qualification expires and is renewable on the assigned date.

Renewal dates may be reassigned to provide benefits to the Laboratory and/or EP. If a renewal date is changed, the Laboratory will be notified in writing of the change.

When qualification is granted, the EP provides a *Certificate of Qualification* to the Laboratory which includes:

a. The name and address of the Laboratory that has been qualified;
b. The Laboratory's Authorized Representative;
c. The effective and the expiration dates of the qualification.

2.11.2 Interim Qualification

Interim Qualification is provided to any Applicant Laboratory that meets the following conditions:

- Approved by the EP to perform as a Laboratory for at least 6 months prior to release of this document, scope of NVLAP accreditation must include all electronically testable categories within 3 months;
- Successfully completed all requirements in this procedure except for 3.1. Requirement 3.1 is to be met within 3 months of receiving interim certifications.

Interim qualification is valid for a maximum of 6 months. When interim qualification is granted, the EP provides an *Interim Certificate of Qualification* to the Laboratory which includes:

a. The name and address of the Laboratory that has been qualified;
b. The Laboratory's Authorized Representative;
c. The effective and the expiration dates of the interim qualification.

2.12 Renewal of Qualification

Each qualified Laboratory receives a renewal application package before the expiration date of its qualification to allow sufficient time to complete the renewal process.

On-site assessments of currently qualified Laboratories are performed in accordance with the procedures in Section 2. If nonconformities are found during the assessment of a qualified Laboratory, the Laboratory must submit a satisfactory response concerning resolution of

nonconformities within 10 days of notification or face possible suspension or revocation of qualification.

2.13 Monitoring Visits

In addition to regularly scheduled assessments, monitoring visits may be conducted by EP at any time during the qualification period. They may occur for cause or on a random selection basis. While most monitoring visits will be scheduled in advance with the Laboratory, EP may conduct unannounced monitoring visits.

The scope of a monitoring visit may range from checking a few designated items to a complete review. The assessors may review nonconformity resolutions; verify reported changes in the Laboratory's personnel, facilities, or operations; or administer proficiency testing, when appropriate.

2.14 Suspension of Lab Qualification

If it is determined that a qualified Laboratory does not comply with the conditions for qualification, EP may suspend the Laboratory's qualification. That determination may be made by EP (e.g., based on evidence obtained during the assessment process) or by the Laboratory (e.g., by notifying EP [via written correspondence] of a major change in writing). Suspension can be for all or part of a Laboratory's qualification. Depending on the nature of the issues involved, EP may also propose to revoke qualification.

If a Laboratory's qualification is suspended, EP notifies the Laboratory of that action, stating the reasons for and conditions of the suspension and specifying the action(s) the Laboratory must take to have its qualification reinstated. A reassessment of the Laboratory may also be required for reinstatement. Conditions of suspension include prohibiting the Laboratory from using the EP symbol on its documentation, correspondence, and advertising during the suspension period in the area(s) affected by the suspension.

The EP will not require a suspended Laboratory to return its Certificate of Qualification, but the Laboratory shall refrain from using the EP symbol in the area(s) affected until such time as the problem(s) leading to the suspension has been resolved. When qualification is reinstated, EP will authorize the Laboratory to resume testing or calibration activities in the previously suspended area(s) as a qualified Laboratory.

2.15 Denial or Revocation of Qualification

If EP proposes to deny or revoke qualification of a Laboratory, EP informs the Laboratory of the reasons for the proposed denial or revocation and the procedure for appealing such a decision. Revocation will be for all EP evaluations performed by the Laboratory.

The Laboratory has 10 days from the date of receipt of the proposed denial or revocation letter to appeal the decision to the Deputy Administrator, Office of Technology Strategy, GSA Office of Government-wide Policy. If the Laboratory appeals the decision, the proposed denial or revocation will be stayed pending the outcome of the appeal. The proposed denial or revocation will become final through the issuance of a written decision to the Laboratory in the event that the Laboratory does not appeal the proposed denial or revocation within the 30-day

period. If qualification is revoked, the Laboratory may be given the option of voluntarily terminating the qualification (see 2.1.16).

A Laboratory whose qualification has been revoked shall cease use of the EP symbol on any of its reports, correspondence, or advertising related to the area(s) affected by the revocation. If the revocation is total, the EP will instruct the Laboratory to return its Certificate of Qualification and to remove the EP symbol from all test or evaluation reports, correspondence, and advertising. If the revocation affects only some, but not all of the items listed on a Laboratory's Scope of Qualification, the EP will issue a revised Scope that excludes the revoked area(s) in order that the Laboratory might continue operations in qualified areas.

A Laboratory, whose qualification has been denied or revoked, may reapply (see 3.1) and be qualified if the Laboratory:

a. Completes the assessment and evaluation process; and
b. Meets the EP conditions for qualification.

2.16 Voluntary Termination of Qualification

A Laboratory may at any time terminate its participation and responsibilities as a qualified Laboratory by advising the EP in writing of its desire to do so. Upon receipt of a request for termination, the EP will terminate the Laboratory's qualification, notify the Laboratory that its qualification has been terminated, and instruct the Laboratory to return its Certificate of Qualification and to remove the EP symbol from all test and calibration reports, correspondence, and advertising.

A Laboratory whose qualification has been voluntarily terminated may reapply (see 3.1) and be qualified if the Laboratory:

a. Completes the assessment and evaluation process; and
b. Meets the EP conditions for qualification.

2.17 Appeals

A Laboratory has the right to appeal any adverse decision made by the EP. Such decisions include refusal to accept an application; refusal to proceed with an assessment; corrective action requests; changes in scope of qualification; decision to deny, suspend, or revoke qualification; and any other action that impedes the attainment of qualification. Appeals are handled by the next higher level in the organization. Appeals of decisions made by the EP Program Managers (e.g., acceptance of an application, corrective action requests) are directed to the Deputy Administrator, Office of Technology Strategy, GSA Office of Government-wide Policy. In some cases, an advisory panel of experts may be called to address appeals of a technical nature.

3 Qualification Requirements

3.1 EP Specific

3.1.1 The Lab shall conduct a System Security Plan in accordance with the controls found in NIST Special Publication 800-53

3.1.2 A small Lab (self declared) shall staff at a minimum: one (1) Lab Director, one (1) Relationship Manager [can be the same as a Lab Director], one (1) Lab Team Lead, one (1) Lab Engineer [can be the same as a Lab Team Lead].

3.1.3 A medium Lab (self declared) shall staff at a minimum one (1) Lab Director, one (1) Relationship Manager, one (1) Lab Team Lead, two (2) Lab Engineers.

3.1.4 A large Lab (self declared) shall staff at a minimum; one (1) Lab Director,

3.1.5 One (1) Relationship Manager, two (2) Lab Team Leads, three (3) Lab Engineers.

3.1.6 The Lab Director shall ensure the responsibilities of the role are fulfilled by the said person, as per Section 3.2.1 of the Lab Specification

3.1.7 The Lab Director shall meet the qualification and training requirements as per Section 3.2.1.1 of the Lab Specification

3.1.8 The Relationship Manager shall ensure the responsibilities of the role are fulfilled by the said person, as per Section 3.2.2 of the Lab Specification

3.1.9 The Relationship Manager shall meet the qualification and training requirements as per Section 3.2.2.1 of the Lab Specification

3.1.10 The Lab Team Lead(s) shall ensure the responsibilities of the role are fulfilled by the said person, as per Section 3.2.3 of the Lab Specification

3.1.11 The Lab Team Lead(s) shall meet the qualification and training requirements as per Section 3.2.3.1 of the Lab Specification

3.1.12 The Lab Engineer(s) shall ensure the responsibilities of the role are fulfilled by the said person, as per Section 3.2.4 of the Lab Specification

3.1.13 The Lab Engineer(s) shall meet the qualification and training requirements as per Section 3.2.4.1 of the Lab Specification

3.1.14 The Relationship Manager shall ensure, at appropriate times, that the Applicant is knowledgeable of their responsibilities as per Section 3.2.5.1 of the Lab Specification

3.1.15 The Lab shall furnish accurate engineering blueprints of the facility, obtained from the building staff

3.1.16 The Lab shall contain one (1) network and telephone closet, minimum of 4x4 feet in size

3.1.17 The Lab shall contain one (1) men's and one (1) women's bathroom, at a minimum

3.1.18 The small Lab shall allocate one (1) reception area, minimum of 8x10 feet in size, one (1) testing area in one (1) office, minimum of 10x10 feet in size, for Lab Staff, one (1) conference

area, minimum of 12x15 feet in size, one (1) storage area, minimum of 5x7 feet in size, and contain one (1) break area, minimum of 7x10 feet in size.

3.1.19 The medium Lab shall allocate two (2) testing areas in two (2) offices, minimum of 10x10 feet in size, for Lab Staff, one (1) conference area, minimum of 12x15 feet in size, one (1) storage area, minimum of 5x7 feet in size, and contain one (1) break area, minimum of 10x15 feet in size

3.1.20 The large Lab shall allocate three (3) testing areas in three (3) offices, minimum of 10x10 feet in size, for Lab Staff, one (1) conference area, minimum of 15x18 feet in size, one (1) storage area, minimum of 7x7 feet in size, and contain one (1) break area, minimum of 12x15 feet in size.

3.1.21 The Lab shall provide one (1) workstation (desktop or laptop) per Lab Employee

3.1.22 The Lab shall implement a LAN available to staff, Stakeholders and Suppliers. Secure WiFi (WPA or greater) may be used in place of a wired LAN.

3.1.23 The Lab shall implement a Lab-wide telephone system that includes voicemail, transfer, hold and speakerphone features.

3.1.24 The Lab shall provide a phone jack for the maximum number of persons planned in each area.

3.1.25 Lab personnel shall have one (1) telephone and telephone number assigned to him/her

3.1.26 The Lab shall implement a speakerphone system in the conference room

3.1.27 The Lab shall implement a fax machine in a central location

3.1.28 The Lab shall implement one (1) high-speed, high-volume printer in a central area, connected to the LAN to allow access by all individuals connected to the LAN

3.1.29 The Lab shall implement a low-end printer in each Lab staff office and Supplier/Stakeholder office to protect printing of confidential information

3.1.30 The Lab shall supply two (2) desks, two (2) chairs, one (1) small locking file cabinet, one (1) wastebasket, and one (1) whiteboard per Lab Staff office

3.1.31 The Lab shall supply one (1) 3x5 foot table and one (1) chair per testing area

3.1.32 The Lab shall supply one (1) table, four (4) chairs, one (1) overhead projector and screen and one (1) whiteboard per conference room

3.1.33 The Lab shall supply one (1) desk, one (1) receptionist chair, one (1) table for fax and printer, and two (2) visitor chairs per reception area

3.1.34 The Lab shall supply shelving and/or one (1) tall locking cabinet (industrial strength) per storage area

3.1.35 The Lab shall supply one (1) table and four (4) chairs per break room

3.1.36 The Lab shall supply one (1) router, one (1) patch panel, one (1) Internet service connection box, one(1) rack to hold equipment – or as needed

3.1.37 The test workstation shall run the Windows XP Operation System with Service Pack 2

3.1.38 The test workstation shall have configured:

- One serial port
- One USB port
- JAVA Runtime Edition v5.0
- Monitor
- Keyboard
- Mouse

3.1.39 The test workstation shall support one reference contact smart card reader supporting T=0 and T=1

3.1.40 The test workstation shall support one reference contactless smart card reader supporting Type A and Type B interfaces

3.1.41 The test workstation shall be compatible with the reference P

3.1.42 The test workstation shall run the Windows XP Operation System with Service Pack 2

3.1.43 The test workstation shall have configured:

- One serial port
- One USB port
- PC Card Type II Slot
- JAVA Runtime Edition v5.0
- Monitor
- Keyboard
- Mouse"

The test workstation shall be compatible with the following reference PIV Cards:

- Contact T=0 only
- Contact T=1 only
- Contactless Type A only
- Contactless Type B only

3.1.44 The test workstation shall be configured with a serial (25 pin to 9 pin) converter

3.1.45 The breakout box shall be implemented as per the specifications of Section 3.3.5.3 in the Lab Spec

3.1.46 The Lab shall employ a process and procedure that encompasses discovery, tracking, and reconciliation of assets over time (i.e. an Inventory List). See Section 4.5 of the Lab Specification for three suggestions for asset tracking

3.1.47 The Lab shall provide adequate power for operation of the Lab and it's electronic loads

3.1.48 The Lab shall provide adequate HVAC systems to properly keep the Lab at optimal temperatures for work in the Lab as well as performance of the various equipment used.

3.1.49 The Lab shall provide adequate lighting for each Lab area

3.1.50 The Lab shall utilize raised floors and/or raised ceiling to facilitate the running of wires and cables throughout the Lab

3.1.51 The Lab shall utilize a fire suppression system that is adequate to prevent destruction of Lab equipment by fire and smoke

3.1.52 The Lab shall employ signage at various locations in and around the Lab indicating each designated area of the Lab

3.1.53 The Lab shall employ signage outside of the Lab to ensure that visitors can easily find the Lab

3.1.54 The Lab shall have installed, industrial strength carpeting wherever carpet is present in the Lab

3.1.55 The Lab shall mitigate the risk of static shock from Lab Staff walking on carpeted areas within the Lab

3.1.56 The Lab shall maintain a freshly painted, clean, professional appearance throughout the Facility

3.1.57 The Lab shall ensure that a sufficient number of IP addresses have been allocated for computer access to LAN resources

3.1.58 The Lab shall be connected to the Internet via a high-speed connection

3.1.59 The Lab's LAN is entirely behind a network firewall, to limit public Internet exposure of the LAN

3.1.60 The Lab shall have a dedicated area for network connectivity related equipment. This area shall be secure and accessible to authorized Lab personnel only

3.1.61 The Lab shall require all visitors to sign in at the reception area

3.1.62 The Lab shall require all visitors to sign out at the end of visit

3.1.63 The Lab shall indicate the visitors name, company and date on the badge assigned to visitors

3.1.64 The Lab shall escort visitors at all times throughout the Facility

3.1.65 The Lab shall collect the visitor's badge at the end of the visit

3.1.66 The Lab shall develop and provide a formal sanctions process for personnel failing to comply with the information security policies and procedures

3.1.67 The Lab shall control all physical access points to the Lab's Facilities

3.1.68 The Lab shall keep current, the list of personnel with authorized access to the Facility, the Lab's information systems, as well as the supplier submissions.

3.1.69 The Lab shall maintain a visitor's log that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name of the person visited

3.1.70 The Lab shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of all information and test systems

3.1.71 The Lab employs automatic emergency lighting systems that activate in the event of power outage.

3.1.72 The Lab monitors and maintains, acceptable levels of temperature and humidity in the Facility

3.1.73 The Lab shall protect all equipment from water damage

3.1.74 The Lab shall conduct daily incremental and weekly full backups of user-level system information and supplier related information

3.1.75 The Lab shall have an alternate storage site for storing of backed up system information

3.1.76 The Lab shall store all backups in an off-site location with protections consistent with (or better than) the security controls described in Section 3.3.10.3.1 of the Lab Specification

3.1.77 The Lab shall employ a mechanism which allow information systems to be recovered and reconstituted to the system's original state

3.1.78 The Lab shall schedule, perform and documents routine preventative and regular maintenance of components

3.1.79 If the information system or component of the system requires off-site repair, the Lab shall remove all information from associated media

3.1.80 The Lab shall maintain a list of maintenance schedules for serviceable equipment used by the Lab

3.1.81 The Lab shall maintain a list of authorized personnel to perform maintenance on the Lab's information systems

3.1.82 The Lab shall implement a malicious code protection software that includes the capability for automatic updates on all machines residing on the Lab's network used to perform daily activities

3.1.83 The Lab shall implement an antivirus software that includes the capability for automatic updates on all machines residing on the Lab's network used to perform daily activities

3.1.84 The Lab shall subscribe to a service which provides information security alerts/advisories on a regular basis

3.1.85 The Lab shall respond to information security alerts/advisories as provided by the service

3.1.86 The Lab shall implement a spam and spyware protection software on all machines residing on the Lab's network used to perform daily activities

3.1.87 The Lab shall ensure that only authorized Lab personnel have access to information in printed form or on digital media

3.1.88 The Lab shall sanitize or destroy media before its disposal or release for reuse

3.1.89 The Lab shall ensure all personnel are exposed to basic information system security awareness before authorizing access to any of the Lab's system

3.1.90 The Lab's information systems shall uniquely identify and authenticate Lab personnel. Authentication may be based on passwords, tokens, biometrics, or multifactor authentication

3.1.91 The Lab shall manage information system accounts including establishing, activating, modifying, reviewing, disabling, and removing accounts

3.1.92 The Lab shall grant access to its information system based on a valid need to know and intended use of the system

3.1.93 The Lab shall ensure that system administrators are notified to disable user accounts upon termination or transferring of any staff personnel

3.1.94 The Lab shall ensure that a record is kept of all information related to evaluations, including but not limited to: forms, contracts, work sheets, workbooks, check sheets, work notes, supplier documentation and feedback

Appendix A – Rules of Behavior

C-1. INTRODUCTION

All EP Lab staff shall follow the following rules of behavior. The rules delineate responsibilities of, and expectations for all individuals for EP Lab purposes. Non-compliance of these rules may result in denial of access to EP Lab systems and resources, and/or other actions that are commensurate with the non-compliance activity.

C-2. ACCESS

- Only use data for which you have been granted authorization.
- Do not retrieve information for someone who does not have authority to access the information, only give information to personnel who have access authority and have a need to know for their EP Lab jobs.
- Do not access, research, or change any file, directory, table, or record not required to perform your OFFICIAL duties.

C-2.1 Account Registration

- Each lab employee shall apply for their own user id for accessing the EP Web Tool.

C-2.2 Logging On to the EP Web Tool

- Each lab employee shall only login to the EP Web Tool using their own user id.

C-2.3 Information Accessibility

- The lab shall restrict access to government and proprietary commercial information. Lab employees shall only have access to that information required to perform their EP lab duties.

C-3. JOB PERFORMANCE

C-3.1 Accountability

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Prevent access to PCs (e.g., initiate password based screen saver) whenever you leave the vicinity of your PC.
- Logout of the EP Web Tool whenever you leave the vicinity of your PC.

C-3.2 Confidentiality

- Be aware of the sensitivity of electronic and hardcopy information, and protect it accordingly.
- Do not allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store hardcopy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media, prior to reusing or disposing of the media.

C-3.3 Integrity

- Protect EP equipment against viruses and similar malicious programs.
- Observe all software license agreements. Do not violate Federal copyright laws.
- Do not install or use unauthorized software on EP equipment. Do not use freeware, shareware or public domain software without your manager's permission and without scanning it for viruses first.
- Observe all software license agreements. Do not violate Federal copyright laws.
- Follow industry standard procedures for maintaining and managing EP Lab hardware, operating system software, application software, and/or database software and database tables.

C-3.4 Passwords

- Protect your password(s) from disclosure. You are responsible for any EP Web Tool activity associated with your user ID and password.
- Do not share your password with others or reveal it to anyone. If there is an operational need to do so, immediately change the password after the need has passed.
- Do not post your password in your work area or hard code it into script.
- Do not use another person's user ID and password.
- Change your password if you think your password is known by an unauthorized individual.
- NEVER give your password out over the phone.
- Be alert to others who may try to obtain your password. Sometimes hackers pose as a system administrator. A hacker may randomly call a user and say that something is wrong on the system to get arbitrary access to your system. They may tell you that they need your password in order to issue you a new one. Always remember that system administrators DO NOT need your password in order to issue you a new password.
- Do not write down your password(s). Memorize them using easy to remember phrases.
- Do not re-cycle passwords by changing them at the required interval and using a few of them over and over in turn, or making minor changes to passwords by adding a number to the base password (e.g., password is changed to password1, password1 is changed to password2).

C-3.5 Reporting

- Contact and inform the Lab Director that you have identified an IT security incident.
- NEVER assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once.
- Seek assistance and/or challenge unescorted strangers in areas wherever EP equipment or information is being used.

C-3.6 Session Time Out

- EP Lab staff shall utilize a screen saver with password protection set to suspend operations at no greater than 15-minutes of inactivity. This will prevent inappropriate

access and viewing of any material displayed on your screen after some period of inactivity.

C-3.7 Backups

- Make backups of PCs files on a regular, defined basis.
- Store backups in a secure environment.

C-3.8 Test Equipment

- Avoid placing EP test equipment near obvious environmental hazards (e.g., water pipes).
- Do not eat or drink near EP test equipment.
- Keep an inventory of all EP test equipment.
- Keep records of maintenance/repairs performed on EP Test equipment.

C-3.9 Awareness

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to hardware and software.

SIGNATURE/ATTESTATION:

I hereby claim that I am authorized to sign this form acting as the _____(lab specification role), for the _____(applicant Lab) I acknowledge that l have read the requirements of the Rules of Behavior (stated above), and I agree to adhere to the above Rules of Behavior. I am also aware that any false claims to this statement could result in a penalty as defined by the maximum extent of federal law.

Name:	
Title:	
Role:	
Signature:	

Appendix B – Conditions for Qualification

CONDITIONS FOR QUALIFICATION

To become qualified and maintain qualification, a laboratory shall agree in writing to comply with the GSA FIPS 201 EVALUATION PROGRAM conditions for qualification. The laboratory's Authorized Representative (C level, President, or Vice President) shall sign this form to attest that the information in the application is correct and to commit the laboratory to fulfill the following conditions:

a) comply at all times with the GSA FIPS 201 EVALUATION PROGRAM requirements for qualification as set forth in FIPS 201 Evaluation Program - Laboratory Qualification Procedures & Requirements and relevant technical documents;
b) fulfill the qualification procedure, especially to receive the assessment team, to pay the fees charged to the applicant laboratory whatever the result of the assessment may be, and to accept the charges of subsequent maintenance of the qualification of the laboratory;
c) participate in completing mock evaluation;
d) resolve all nonconformities;
e) report to GSA FIPS 201 EVALUATION PROGRAM within 30 days any major changes that affect the laboratory's:
— legal, commercial, organizational, or ownership status,
— organization and management; e.g., key managerial staff,
— policies or procedures, where appropriate,
— location,
— personnel, equipment, facilities, working environment or other resources, where significant,
— Authorized Representative or Approved Signatories, or
other such matters that may affect the laboratory's capability, or compliance with the requirements of the FIPS 201 Evaluation Program Laboratory Qualification Procedures & Requirements and relevant technical documents.

SIGNATURE/ATTESTATION:

I hereby claim that I am authorized to sign this form on behalf of the _____ (applicant Lab). I acknowledge that l have read the CONDITIONS FOR QUALIFICATION (stated above), and I agree to adhere to them I am also aware that any false claims to this statement could result in a penalty as defined by the maximum extent of federal law.

Name:	
Title:	
Signature:	